MCOLES

Michigan Commission on Law Enforcement Standards

MCOLES Information and Tracking Network (MITN)

SECURITY POLICY

ADOPTED DATE:

September 11, 2003

EFFECTIVE DATE:

September 11, 2003

Version 1.0

1.0 POLICY STATEMENT

The Michigan Commission on Law Enforcement Standards (MCOLES) has created the MCOLES Information and Tracking Network (MITN) to provide criminal justice agencies with a secure and efficient system to comply with the requirements of Public Act 203 of 1965, as amended, Public Act 302 of 1982, as amended, relevant Administrative Law, and MCOLES operational policy and procedures. This security policy requires that users maintain respect for the privacy of confidential information at all times. A cooperative effort among all users is necessary to prevent misuse, eliminate the risk of liability, and promote the efficient use of MITN as an information technology resource and service.

2.0 PURPOSE

The purpose of this policy is to define and specify the requirements for access to, and use of the MITN system. It also specifies the use and dissemination of information obtained from the use of the MITN system.

3.0 ENTITIES AFFECTED BY THIS POLICY

3.1 All agencies designated as registered entities by MCOLES as User Agencies in the MITN system.

3.2 All MITN Operators designated as such by the User Agency and authorized by the MCOLES to access the MITN system for its intended purposes.

3.3 Authorized MCOLES staff.

3.4 State of Michigan system and network administrators.

3.5 Vendors under contract to the state of Michigan and the MCOLES responsible for system maintenance and administration.

4.0 SECURITY ROLES AND RESPONSIBILITIES

4.1 The MCOLES shall set and maintain policies, procedures, and user guides for access, use, and security of the MITN system. All MCOLES authorized User Agencies and Operators shall comply with, and remain in compliance with, the MITN Security Policy, procedures, system user guides, and operational memos published by the MCOLES.

4.2 The MCOLES staff shall enforce the MITN Security Policy, procedures, system user guides and published operational memos. This shall be done by conducting field inspections of MITN user sites as provided for in administrative law and in this policy.

4.3 The MCOLES is responsible for MITN security control. Security control includes, but is not limited to, establishing and implementing policies, procedures, system use guides and use memos governing:

4.3.1 Operation of the MITN system;
4.3.2 Creation and submission of information;
4.3.3 Dissemination and use of information obtained from the MITN system;
4.3.4 Retention and disposal of information obtained using the MITN system; and
4.3.5 Referral of violations to the appropriate Prosecuting Attorney.

4.4 Total network security is the shared responsibility of all MITN application and system users and operators.

5.0 SECURITY REQUIREMENTS

To qualify for MITN access, each User Agency and Operator must agree to, and implement, the following security requirements.

5.1 The User Agency head must agree to the requirements of this security policy by completing and submitting a User Agency Agreement before access will be granted to the agency.

5.2 User Agencies shall be responsible for the security of and access to the MITN system and information obtained using MITN. This includes all information that is viewed, printed or submitted to the MCOLES using MITN.

5.3 User Agencies shall be responsible for ensuring the secure operation of the local network workstation, stand-alone personal computer, or laptop computer used to access the MITN system. Operating practices, that expose the MITN system to security incidents, may be cause for revocation of User Agency and/or Operator access rights.

5.4 Requests for access rights for individual agency Operators shall only be made by the User Agency head or the agency head's designated single point of contact.

5.5 Requests made by a designated User Agency single point of contact shall only be accepted after written notice of such designation from the User Agency head has been received and verified by the MCOLES.

5.6 To qualify for MITN access, an Operator Agreement is required for each agency employee for whom the User Agency Head is seeking MCOLES authorization to access the MITN system. Each applicant for an Operator Agreement must disclose all information relevant to compliance with the MITN security policy.

5.7 Access shall not be requested or granted if the Operator is a fugitive from justice or has ever been convicted of:

5.7.1 Any felony or any offense punishable by more than 1 year;
5.7.2 Any crime involving fraud or misappropriation;
5.7.3 Any crime of misuse of computer systems or information.

5.8 If a determination is made by MCOLES that MITN access by the Operator applicant would not be in the public interest, such access will be denied and the Operator applicant's User Agency shall be notified in writing of the access denial.

5.9 The User Agency head must report any changes in the status of Operators or previous User Agency head within three working days of the change becoming effective.

5.10 Operators who are charged or convicted of any of the items in 5.7 above after obtaining secure access to the MITN system must be reported to the MCOLES. This may result in revocation of the Operator's MITN access rights.

5.11 Operators shall access MITN only for those purposes and to the extent for which they are authorized. Sanctions for access violations may be applied to the Operator(s) and/or User Agency. An Operator's authorized access is that which is expressly stated on the Operator Agreement.

5.12 Operators shall maintain the security of their own unique user ID and password. These are issued only by MCOLES to each authorized Operator and cannot be shared by the Operator with other members of the user agency even if the user agency member is also an authorized Operator. User Agency members not specifically authorized by the MCOLES as Operators shall not be allowed to access the MITN system. Operators may only access the MITN system with the ID and password issued to them.

5.13 Specific physical security standards shall be met where Operators access the MITN system. The site at which a computer is being used to access the MITN system shall have adequate physical security to protect against any unauthorized viewing or access to the system. Such sites shall include any location where Operators use a personal computer, laptop computer or network workstation to access the MITN system.

5.14 Operators shall log out of MITN when leaving a computer or workstation not located within a secure area of the User Agency's facilities. This requirement includes fully closing the browser window that was opened to access the MITN system.

5.15 Operators must blank the screen of the personal or laptop computer or a network workstation in a secure area at the User Agency site when the Operator is away from the computer or workstation. At a minimum, this shall be done by use of a password-protected screensaver.

5.16 The use of a wireless connection for accessing the MITN system is prohibited.

5.17 User Agencies and Operators shall immediately implement any updates, additions or revisions to policies, procedures, system user guides or operational memos published by the MCOLES

6.0 DISSEMINATION OF MITN INFORMATION

6.1 The information submitted to and maintained in the MITN system is documented criminal justice information and shall be protected to ensure correct, legal, and efficient dissemination and use.

6.2 An authorized Operator receiving a request to submit information to MITN, or produce information using MITN, shall ensure that the person requesting the information is authorized to receive the information. An unauthorized request for, or receipt of such material may result in criminal proceedings. Authorized use of MITN information is governed by Public Act 203 of 1965, as amended, Public Act 302 of 1982, as amended, related administrative law, and MCOLES policy.

6.3 Information obtained from MITN and documents produced by the use of MITN shall be used only for the purpose for which that request was made. Upon request by MITN system administrators or MCOLES inspectors, User Agencies and individual Operators must provide a valid reason for all inquiries. Access to MITN may be revoked if information is disseminated to persons without authority to receive it. Authority to receive MITN information may extend to the User Agency, employing governmental unit or service providers under contract to the User Agency.

6.4 Documents produced by use of the MITN system shall be maintained in a secure records environment.

6.5 All unauthorized dissemination of information obtained from the MITN system is prohibited.

7.0 MITN SYSTEM SITE INSPECTIONS

7.1 All User Agencies having access to MITN shall permit MCOLES inspections. This includes but is not limited to making appropriate inquiries with regard to the proper operation of the MITN system in compliance with controlling statutes, administrative law, this Security Policy, MCOLES policies and procedures, system user guides and operational memos.

7.2 All User Agencies having access to MITN shall permit MCOLES staff to conduct appropriate inquiries with regard to allegations of security violations.

8.0 SANCTIONS

8.1 Failure to comply with all of the security requirements of this policy and in the User Agency and Operator agreements may result in revocation of all access rights to the MITN system and/or other penalties, including criminal prosecution.

8.2 Failure by a User Agency or an Operator to comply with the disclosure requirements of this policy, the User Agency Agreement, or the Operator Agreement at the time of application for MITN security access, may result in revocation of all access rights to the MITN system and/or other penalties, including criminal prosecution. This includes but is not limited to concealment or failure to disclose charging or conviction information.

APPENDIX A: DEFINITIONS

The terms and definitions found within this document and related user agency and operator agreements are to be considered in the context of their applicability to the MITN Security Policy. Alternate definitions may exist for environments outside of this policy.

Access: Opportunity to make use of the MITN system. The ability to have contact with a computer or network workstation from which a transaction may be initiated.

Access Control: Procedures and controls that limit or detect access to critical information resources.

Access Device: The end user medium that is used to access MITN.

Access Level: The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users.

Authenticate: Establishing the validity of a claimed user or object.

Authentication: To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. The proof of the unique alphanumeric identifier used to identify an authorized user.
See Identification.

Authorization: The process of MCOLES review of an Operator application to determine what activities an Operator is permitted to perform. An authorized Operator may be authorized for multiple types of use or activity. Technical controls may be implemented to determine authorized actions, but may not fully define or restrict the scope as specified in organizational policy, procedure, or law.

Authorized Access: The ability to perform an authorized transaction or having access to MITN information that is otherwise prohibited by organizational policy or law.

Chief Administrative Officer: The head of a political subdivision; e.g. mayor, chairman of the board of commissioners, city manger, village president, or township supervisor. This will be the Sheriff if only employees of the Sheriff's Office access the MITN system.

Computer: A machine that can be programmed in code to execute a set of instructions (program). In an automated information system, the term *computer* also refers to the components inside the case: the motherboard, memory chips, and internal storage disk(s).

Computer Security: Measures and controls that ensure confidentiality, integrity, and availability of computer assets, including, but not limited to, hardware, software, firmware, and information being processed, stored, and communicated.

Confidential Information: Information maintained by state and local agencies that are exempt from disclosure governed by state or federal laws. The controlling factor for confidential information is dissemination.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Confidentiality Protection: Requirement of access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, and proprietary information.

Criminal Justice Agency: The courts, a governmental agency, or any sub-unit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Training Provider: A criminal justice agency, city, county, township, village, community college, university, state agency, corporation, or individual approved by the Michigan Commission on Law Enforcement Standards to offer training to law enforcement other than the basic law enforcement training curriculum..

Data Integrity: The validity, timeliness, accuracy, and completeness of records.

Denial of Service: The result of any action or series of actions that prevents the MITN system from providing information or other services to authorized users.

Dial-Up: The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Dial-Up Access: Access to system resources via a telephone line and a modem device.

Dial-Up Line: A communications circuit that is established by a switched-circuit connection using the telephone network.

Disclosure: Access to confidential or sensitive information.

Field Inspection: The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Information Security: The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure or dissemination of information whose protection is authorized by executive order or statute.

Inspector: Individual authorized by MCOLES to inspect MITN User Agency sites and records.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Management Control: The authority of MCOLES to set and enforce all of the following:

(1) Priorities;

(2) Standards for the selection, supervision and termination of USER AGENCY and Operator access to MITN; and

(3) Policy governing the operation of computers used to access information insofar as the equipment is used to process, store, or transmit any received information and includes the supervision of equipment, systems design, programming and operating procedures necessary for the development and implementation of MITN.

Michigan Commission on Law Enforcement Standards (MCOLES): The commission formed by Michigan Executive Directive 2001-05, which combined the Commission on Law Enforcement Standards, created by Act No. 203 of the public Acts of 1965 and the Michigan Justice Training Commission, created by Act No. 302 of the Public Acts of 1982.

MITN: The MCOLES Information and Tracking Network. A web-enabled based information system used by authorized User Agencies and Operators to conduct business related to the mandates of the MCOLES.

Modem: Acronym for modulator-demodulator. A device or application that permits a computer to transmit data over telephone lines by converting digital data to an analog signal.

Network: A collection of computers and other devices that are able to communicate or interchange information with each other over a shared wiring configuration. Such components may include automated information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Network workstation: a computer or other access device connected with a User Agency network allowing the Operator to access the Internet.

Operator: an individual employee of a User Agency, identified by the User Agency head or designated single point of contact as a trusted individual who has been authorized by the MCOLES to access the MITN system.

Operator Agreement: A current, signed written agreement with the appropriate signatory authorities that will authorize the provision of said access set forth within the agreement. The agreement refers to the necessary security-related provisions therein.

Password: A protected word or string of characters which, in conjunction with a user identifier (user ID), serves as authentication of a person's identity when accessing the MITN system.

Physical Security: (1) The measures used to provide physical protection of resources against deliberate and accidental threats. (2) The protection of building sites and equipment and information and software contained therein from theft, vandalism, natural and manmade disasters, and accidental damage.

Point of Contact (POC): The User Agency individual identified as the security point-of-contact (POC) for access to MITN.

Recognized Basic Law Enforcement Training Academy: An agency or institution that is approved by the Michigan Commission on Law Enforcement Standards to offer the basic police training program.

Registered Entity: a Criminal Justice Agency or a Criminal Justice Training Provider identified in the MITN system as User Agency.

Related agency: an agency within the governmental unit of the User Agency with whom the User Agency must exchange sensitive information in order to fulfill legal mandates.

Remote Access: Use of modem and communications software to connect to a computer network from a distant location via a telephone line or wireless connection.

Security Control: Hardware, programs, procedures, policies, system user guides, operational memos and physical safeguards that are put in place to assure the integrity and protection of information and the means of processing it. The ability of the MCOLES to set, maintain, and enforce standards for the selection, supervision, and termination of personnel and policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support the MITN system. Related means used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Security Incident: Any act or circumstance that involves MITN data that deviates from the requirements of the MITN Security Policy or state and Federal governing statutes, e.g., compromise, possible compromise, inadvertent disclosure, and deviation.

Security Requirements: Types and levels of protection necessary for a system to maintain an acceptable level of security.

Security Measures: Protective safeguards and controls that are prescribed to meet the security requirements specified for an automated information system. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

Sensitive Information: Information maintained by agencies that require special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. The controlling factor for sensitive information is that of integrity.

Service Provider: an entity that provides screening, research, testing background investigation or other services for a User Agency or the User Agency's governmental unit.

Single Point of Contact: One designated individual responsible for direct communication with the provider regarding security and other interactions with the MITN system.

Standalone System or computer: A system or single computer that is physically and electronically isolated from all other systems and computers. It has no internal network connections and has no ability to share information between a secure and non-secure environment. It is intended to be used by one person at a time, with no data belonging to other users remaining available to the system.

System Integrity: Optimal functioning of the MITN system, free from unauthorized impairment or manipulation.

Unauthorized Access: Obtaining access to an area, system or resource that has been designated for authorized personnel only without such authority expressly conveyed by written agreement. Obtaining access which exceeds such expressed authority.

User Agency: An authorized Michigan criminal justice agency, basic law enforcement training academy, and/or state and national criminal justice training provider which has been authorized by the Michigan Commission on Law Enforcement Standards through an executed User Agency agreement to access the MITN system to exchange information with MCOLES.

User Agency Agreement: A current, signed written agreement with the appropriate signatory authorities that will authorize the provision of said access set forth within the agreement. The agreement refers to the necessary security-related provisions therein.

User Agency Head: The chief, sheriff, director, president, CEO or acting agency head of a User Agency. When the User Agency head position is vacant the chief administrative officer of the local governing unit shall be considered the User Agency head. This shall be the undersheriff in a sheriff's office if only sheriff's employees access the MITN system.

Wireless: A telecommunication path that does not require a landline infrastructure.

MCOLES Information and Tracking Network (MITN)
Web Module Functionality
Agency and Operator Access

Law Enforcement Agency

- Prescreen an individual
- Hire an employed recruit
- Activate the license of an LEO candidate
- Hire a law enforcement officer
  - View employment and training history
- Update an employee's profile
- Change an officer's law enforcement authority
- Separate a law enforcement officer
- Complete annual registration
  - Verify roster of officers; enter annual hours worked
  - Report LED expenditures
  - Register for LED funding
- Add an in-service course
- View and/or update an existing course or course roster
- Search for instructors
- Search for other in-service course offerings (Training Course Registry)
- Look up LERC resources
- Maintain entity profile
- Maintain operator web password

Basic Training Academy

- Create a new session, including adding new courses and exams
- Update a session during the running of the session
- Search for instructors
- Add a new instructor to MITN
- Enroll a new student
- Maintain entity profile
- Maintain operator web password
- Look up LERC resources
- Look up in-service course offerings (Training Course Registry)

In-Service Training Provider

- Add an in-service course
- View and/or update an existing course or course roster
- Search for other in-service course offerings (Training Course Registry)
- Maintain entity profile
- Maintain operator web password

Individual Officer

- View employment and training history
- View profile information
- Create and delete officer's public password
- Maintain officer's web password
- Look up in-service course offerings (Training Course Registry)